



Manual

DA-FormMaker formmail script

Dunkel und Iwer GbR
Gartenstr. 12a
15907 Lübben (Spreewald)

info@ekiwi.de
<https://da-software.net>

Table of Contents

Introduction.....	2
System requirements.....	2
License terms.....	2
Script installation.....	3
Setting up „config.php“.....	3
IP lock.....	4
IP database or text file.....	4
Database access.....	4
Activate log function.....	4
Activate spam filter.....	4
Error pages.....	5
Configuration for sending mail.....	5
Settings captcha.....	6
Upload of the script.....	7
Setup the database.....	7
Assign file permissions.....	8
Error diagnostics.....	9
Spam filter.....	10
Blacklist.....	10
Automatic update of the blacklist.....	11
Link spam.....	12
HTML spam.....	12
Captcha and time check.....	13
Email template customization.....	13

Introduction

In this tutorial we describe the steps to install the formmail script for DA-FormMaker on your own webspace. The installation allows you to run your forms independently.

Problems with the installation of the script / installation service

If you have any questions or problems, please just contact our support:

- <https://da-software.net/en/contact/>

We are also happy to install the script for you. You can find the information about our installation service here:

- <https://da-software.net/support/installationservice-fuer-php-formmail-scripte/>

System requirements

The following system requirements apply to the script:

- PHP 7.4, PHP 8
- MySQL-database (optional)
- Linux / Unix Server (Windows limited support)

License terms

As a buyer of DA-FormMaker software you may use this script without any restrictions. You may install the script on your servers as often as you like. It is also allowed to install and distribute it on customer web servers.

You may modify the script according to your wishes at your own risk, as well as commission third parties to modify the script.

The script and the associated files are sold without any functional guarantee for the hardware or software used in the environment. The risk of the use of the script is incumbent on the licensee, any reimbursements in case of a legal case extend at most to the purchase price of the license. The license can be used for an unlimited period of time.

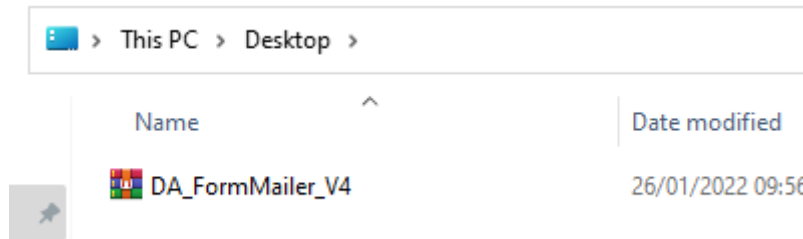
The script contains further open source components, each with its own license (folder vendor).

Script installation

The latest version of the script is available on our website:

<https://secure.da-software.de/DA-FormMaker/index.html>

The download is a ZIP archive. For the installation this must be unpacked.



Setting up „config.php“

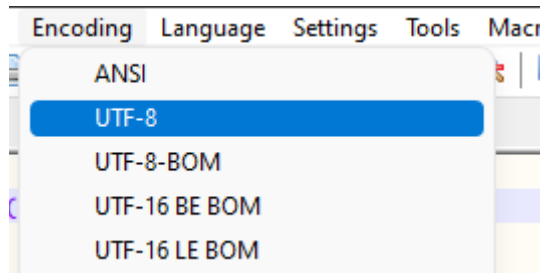
The configuration of the script is done via the file "config.php". Open this with a text editor. An editor like Notepad++ is recommended.

```

1  <?php
2  include_once('_logic/mail.php');
3
4  //-----
5  // Konfiguration IP-Sperre / Configuration IP lock
6  //-----
7  $iplock = 0; //IP-Sperre aktivieren 0 = aus ; 1 = an / IP lock active 0
8  $iplocktime = 60; //Dauer der IP-Sperre in Sekunden / Duration of the ip
9
10 //-----
11 //Verwenden Sie eine Datei oder eine Datenbank für die IP-Sperre, falls
12 //keine Datenbank ist für IP-Sperre als Datei erforderlich
13 //-----

```

When saving, make sure that the file is saved as **UTF-8 file, without BOM**.



Otherwise, errors may occur during script execution. In the file you will find various sections and settings. Also pay attention to the notes in the file.

IP lock

IP blocking checks whether the form has already been sent from an IP address within a specified time. If yes, the form will not be sent again. The lock serves as a protection against mass submission of the form. To enable it, set the value to 1:

```
$iplock = 0; // IP lock active 0 = off ; 1 = on
```

You can also specify the time within which the lock should apply:

```
$iplocktime = 60; // Duration of the ip lock
```

The value is in seconds.

IP database or text file

To use IP blocking, the IP addresses of the users must be stored for the specified time. This can be done either in a MySQL database or in a text file. If you want to use the text file, set the following setting in the "config.php":

```
$conf_iplock_type = IpCheckType::FILE;
```

To use the MySQL database:

```
$conf_iplock_type = IpCheckType::DB;
```

Our recommendation is to use the database, because it allows parallel accesses. Using the text file is recommended only if you cannot use a MySQL database.

Database access

The database is used for captcha and IP lock. If you want to use captcha and IP lock with database, enter the access data here:

```
$dbname = 'formmail'; // database name
$dbhost = 'localhost'; // database server
$dbuser = 'root'; // user name
$dbpass = ''; // password
```

Activate log function

With the log function, the e-mails are additionally stored in the "archiv" folder.

```
$conf_log = 0; //1 = Log active
```

Activate spam filter

Use the following option to enable the spam filter:

```
$conf_antispam = 1;
```

The spam filter analyzes the e-mails and discards spam messages. As a rule, it is recommended to use the spam filter. We will explain the exact function of the spam filter and how to set it up in a later chapter.

If you want to test the function of the spam filter, you can not only discard spam mails, but also send them to your own e-mail address for checking. This is possible with the following setting:

```
$conf_antispam_copy_mail = 1;
$conf_antispam_mail_address = "devnull@ekiwi.de";
```

If the setting is set to "1", spam messages are not discarded but sent to the mail address. This allows you to check if the spam filter is working correctly.

Error pages

Various settings for error pages follow. Partly these pages can be overwritten by the form. If none are specified in the form, these will be used.

```
$IPErrorPage = 'https://www.ekiwi-scripts.de/form/errorpages/blockip.htm';
```

Sets the error page that appears when IP blocking prevents sending.

```
$CaptchaErrorPage = 'https://www.ekiwi-scripts.de/form/errorpages/blockcaptcha.htm';
```

Sets the error page that appears when an invalid captcha has been entered.

```
$FileErrorPage = 'https://www.ekiwi-scripts.de/form/errorpages/blockfile.htm';
```

Sets the error page that appears when the maximum configured file size has been exceeded. You can set the maximum file size with the following setting:

```
$max_attach_size = 5000000;
```

The specification is in bytes. 1 megabyte corresponds to 1048576 bytes.

```
$BlockFilePage = 'https://www.ekiwi-scripts.de/form/errorpages/blockfiletype.htm';
```

The error page for file uploads that are not allowed. By default, all file types are allowed for upload. To allow only certain file types, modify this line:

```
$BlockFileList = array();
```

To allow only certain file types or extensions, specify them in the array:

```
$BlockFileList = array( ".pdf", ".exe", ".doc", ".xls" );
```

Entries are separated by commas and must be specified in quotation marks and periods.

Configuration for sending mail

Another important point is the sending method, you can choose between Sendmail and SMTP:

```
$c_mail_send_type = MailSend::Sendmail;
```

or

```
$c_mail_send_type = MailSend::SMTP;
```

Sendmail sends the emails directly via the web server. This variant requires no further configuration, but has the disadvantage that spam filters sometimes filter out the mails if they come from a rather unknown server.

We recommend the SMTP configuration for this. To do this, you create an SMTP account at your web hoster and then enter the access data in config.php:

```
$c_smtp_host = "localhost"; //Serveraddress
$c_smtp_username = "ihrname@example.com"; //Username
$c_smtp_password = "ihrpasswort"; //Password
```

The transmission is encrypted, if the port differs, it can be set with the following setting:

```
$c_smtp_port = 587;
```

In case of problems with sending e-mails, e.g. mails do not arrive, it may help to define a default sender:

```
$c_standard_mail = "andy.dunkel@ekiwi.de";
```

This e-mail address is then always used as the sender e-mail and should correspond to an existing address belonging to the server or web space.

If problems occur during sending, SMTP debugging can be activated:

```
$c_smtp_debug = true;
```

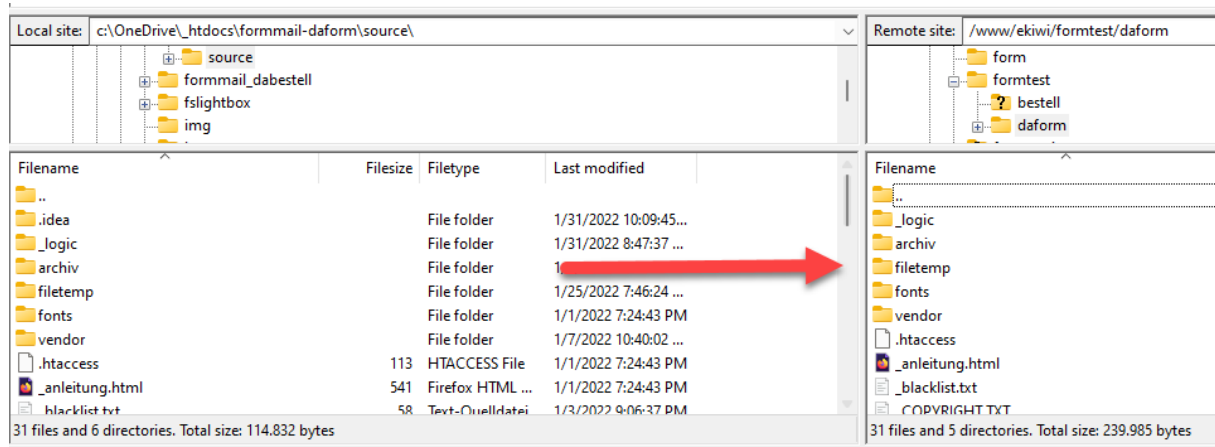
If the setting is set to "true", a detailed output takes place after sending. Error messages and warnings are then output here. For productive operation, the setting must be set to "false" again.

Settings captcha

In this section the captcha can be configured, e.g. number of glitches, colors etc.. The details can be found in the "config.php".

Upload of the script

After you have finished configuring the script, you can transfer the script to your web space using an FTP program.



Setup the database

If you want to use the Captcha function or the IP lock is configured for MySQL, you must now set up the MySQL tables. To do this, create a MySQL database in the admin area of your web host. Then call the installation of the formmail script in the browser by calling the "sqlinstall.php" file of the script.

https://yourserver.de/pfad/formmail_v4/sqlinstall.php

Installation MySQL-Tabellen / Installation MySQL tables

Zugangsdaten für MySQL / Credentials for MySQL:

Datenbankserver / Server name:

Datenbankname / Database name:

Benutzername / User name:

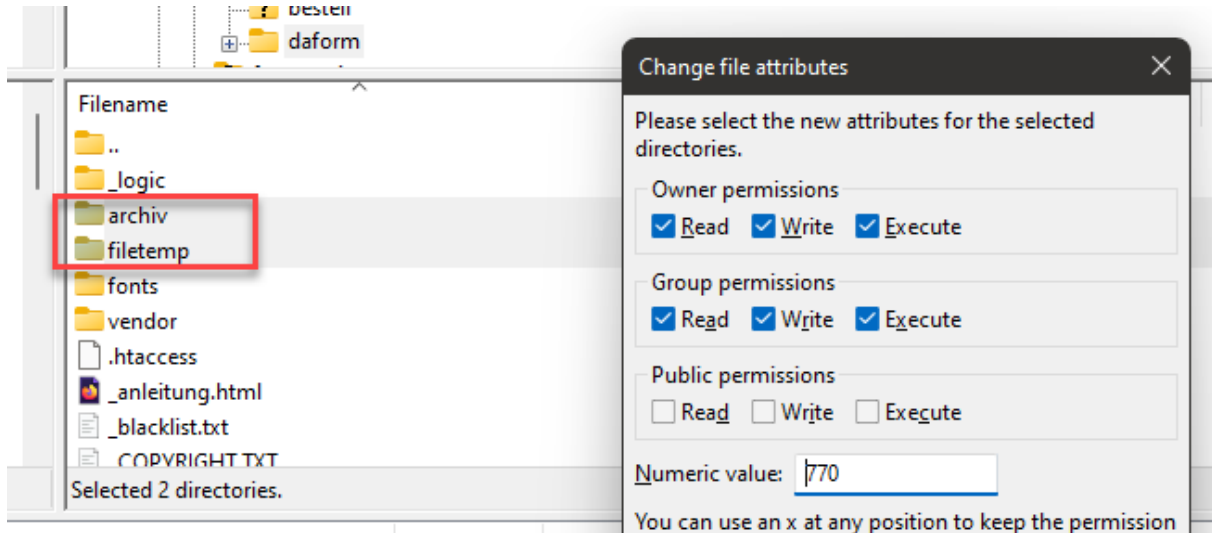
Passwort / Password:

Enter the access data to the database and click on "Install tables". The tables will now be created in the database. It is recommended to delete the file "sqlinstall.php" from the webspace after the setup.

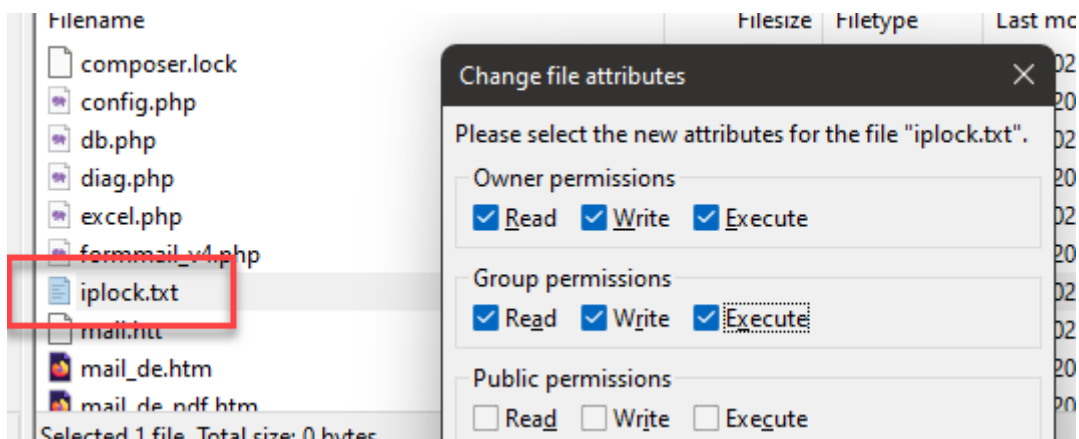
Assign file permissions

If your forms use file uploads, the "filetemp" folder must have write permissions for the script. The "archiv" folder also needs write permissions if the archive function is enabled.

The following setting is exemplary and depends on the configuration of your web hoster:

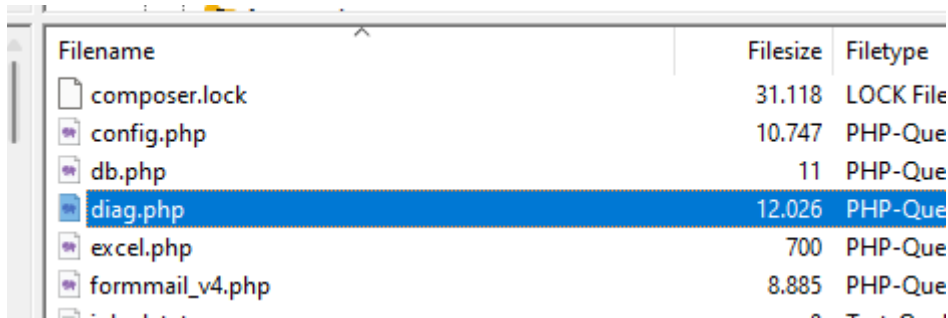


Provided that you have set up the IP lock as a file, the "iplock.txt" file also requires write permissions.



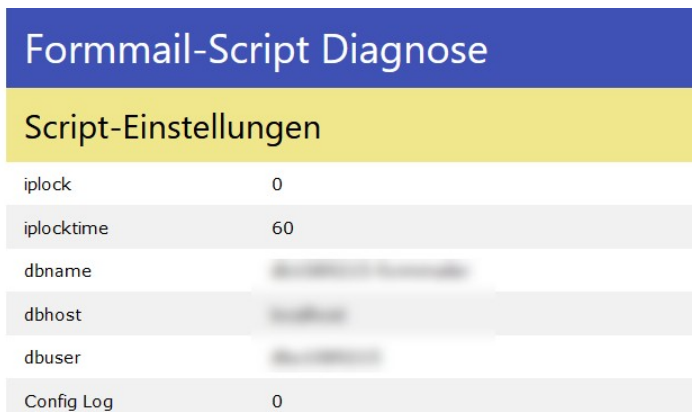
Error diagnostics

If you have problems with the execution of the script, you can activate the diagnostic function, rename the file "diag.____" to "diag.php".



Filename	Filesize	Filetype
composer.lock	31.118	LOCK File
config.php	10.747	PHP-Que
db.php	11	PHP-Que
diag.php	12.026	PHP-Que
excel.php	700	PHP-Que
formmail_v4.php	8.885	PHP-Que

You can then call up this page in the browser. The list contains the current configuration and also shows warnings and errors.



Formmail-Script Diagnose	
Script-Einstellungen	
iplock	0
iplocktime	60
dbname	
dbhost	
dbuser	
Config Log	0

Note: If you have problems with the installation, then activate the diagnostics and send us the link to the diagnostics, along with your request.

Spam filter

If the spam filter is enabled, the following spam filters are activated.

Blacklist

A blacklist or text file can be used to filter e-mails containing certain terms. If an entry appears in the list, the e-mail is filtered. We keep a daily updated spam list for our formmail scripts, which can be downloaded directly from us.

Example of blacklist filtering for "folmax.pw":

Telefon: 030 [REDACTED]
Email: jack [REDACTED]
Frage: Mllscke, Abfallscke alle
 Sorten.
 Gewebescke. Kartoffelscke.
 Laubscke.
 Raschelscke. Zwiebelscke.
 Spnescke.

Hochwertige Waren vom
 Produzent. Fabrikverkauf.
 Versand am gleichen Tag
 aus Frankfurt. Bis 95 %
 gntiger als auf dem Markt.

Arbeitshandschuhe und
 Vieles mehr.

Info auf: folmax.pw

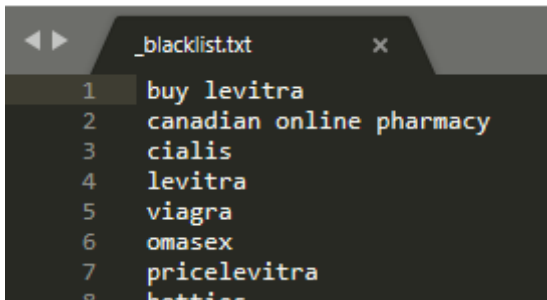
Mit freundlichen Gr

Zustimmung: Aktiviert

The blacklist is kept in the file "_blacklist.txt".

Filename	Filesize	Filetype
fonts		File folder
vendor		File folder
.htaccess	218	HTACCESS ...
_anleitung.html	541	Firefox HT...
_blacklist.txt	125.718	Text-Quell...
_COPYRIGHT.TXT	1.514	Text-Quell...
_version.txt	1.276	Text-Quell...

The file contains the terms that will be filtered for. One term per line:



```

1 buy levitra
2 canadian online pharmacy
3 cialis
4 levitra
5 viagra
6 omasex
7 pricelevitra
8 botties

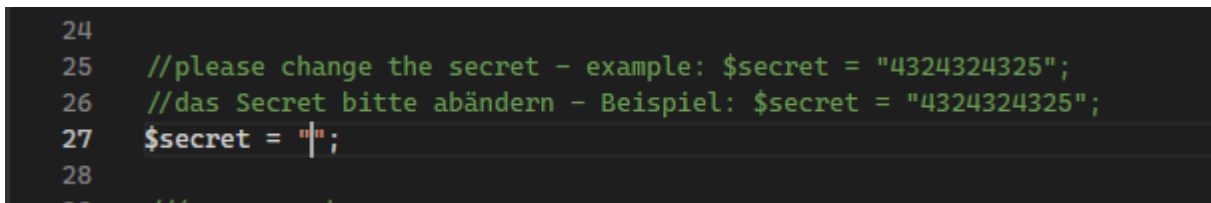
```

We ourselves maintain and update a predefined blacklist with the latest spam terms. You can download this from the following address:

<https://ekiwi-scripts.de/antispam/spam.php>

Automatic update of the blacklist

You can also update the blacklist automatically from our server via the file "update_blacklist.php". First edit the file with a text editor and enter a random secret.



```

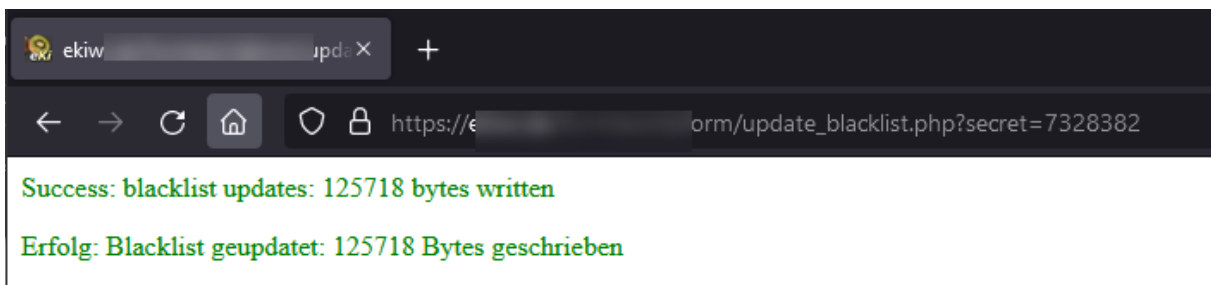
24
25 //please change the secret - example: $secret = "4324324325";
26 //das Secret bitte abändern - Beispiel: $secret = "4324324325";
27 $secret = "|";
28
29 //do not change

```

For security reasons, this must be passed as a parameter when calling the page:

https://yourserver.de/formmail_v4/update_blacklist.php?secret=444555

The file "_blacklist.php" must be assigned write permissions before. Call the file in the browser, the blacklist will now be downloaded and installed.



```

Success: blacklist updates: 125718 bytes written
Erfolg: Blacklist geupdatet: 125718 Bytes geschrieben

```

You can also set up a cron job for automatic updating.

Note: With the automatic update, the file is overwritten with every update. If you additionally want to maintain your own blacklist in parallel, you can use the file "_blacklist_user.txt".

Captcha and time check

Next to the input of the captcha, the captcha also checks the time needed for sending the form. Spam bots usually fill out the form automatically. If the form is submitted in under 3 seconds, the form is viewed as spam.

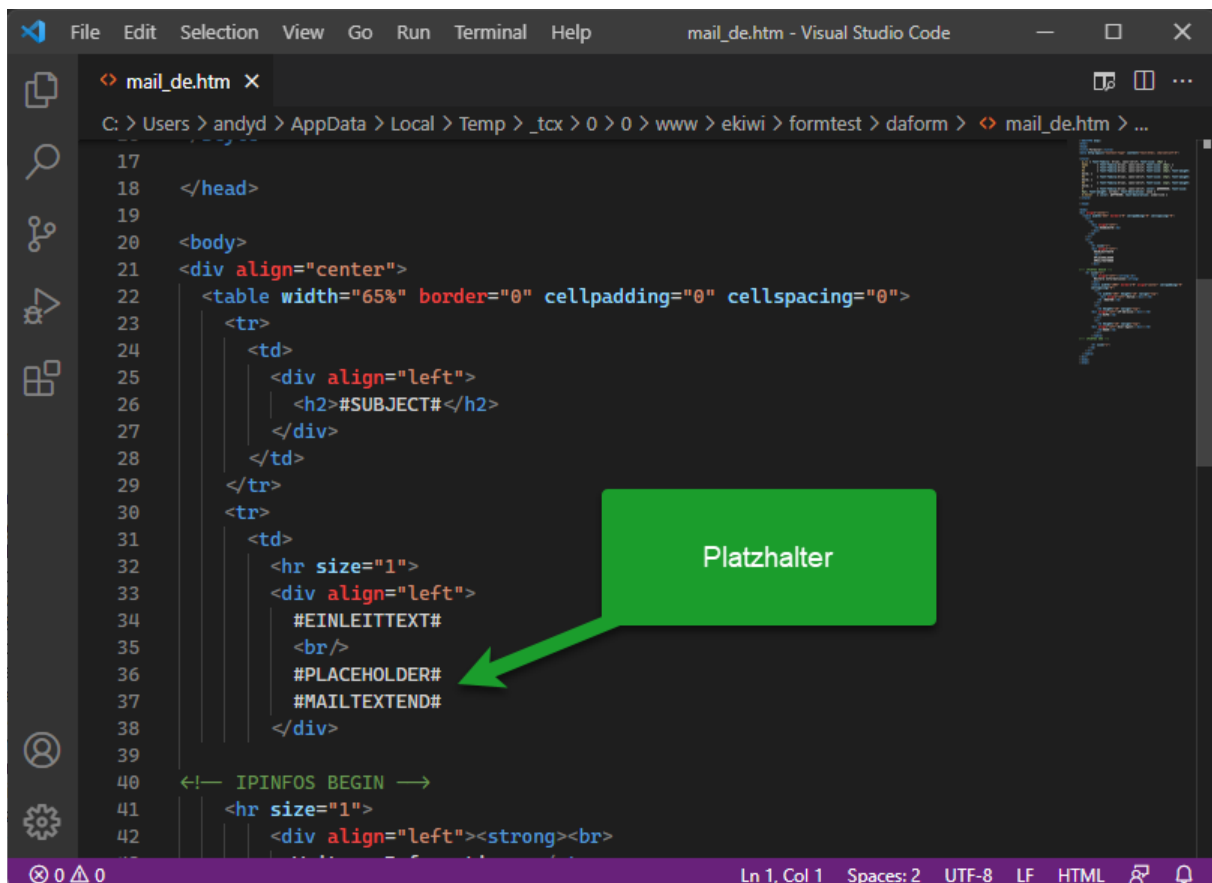
Email template customization

The script contains template files, which are used for the e-mails:

iplock.txt	0	Text-Quell...	02.1
mail.htt	76	HTT-Datei	01.1
mail_de.htm	1.967	Firefox HT...	22.1
mail_de_pdf.htm	3.058	Firefox HT...	22.1
mail_en.htm	1.957	Firefox HT...	22.1
mail_en_pdf.htm	3.052	Firefox HT...	22.1
refresh.png	3.001	FirefoxView D...	01.1

The "mail.htt" is used for text mails. The .htm files are used for sending HTML mails, respectively for creating the PDF document.

Please note that the placeholders are still present so that the emails / PDF are created correctly.



```

17
18 </head>
19
20 <body>
21 <div align="center">
22 <table width="65%" border="0" cellpadding="0" cellspacing="0">
23 <tr>
24 <td>
25 <div align="left">
26 <h2>#SUBJECT#</h2>
27 </div>
28 </td>
29 </tr>
30 <tr>
31 <td>
32 <hr size="1">
33 <div align="left">
34 #EINLEITTEXT#
35 <br />
36 #PLACEHOLDER#
37 #MAILTEXTEND#
38 </div>
39
40 <!-- IPINFOS BEGIN -->
41 <hr size="1">
42 <div align="left"><strong><br>

```